A HIGHER-RANK MERSENNE PROBLEM

GRAHAM EVEREST, PETER ROGERS, AND THOMAS WARD

Abstract. The classical Mersenne problem has been a stimulating challenge to number theorists and computer scientists for many years. After briefly reviewing some of the natural settings in which this problem appears as a special case, we introduce an analogue of the Mersenne problem in higher rank, in both a classical and an elliptic setting. Numerical evidence is presented for both cases, and some of the difficulties involved in developing even a heuristic understanding of the problem are discussed.

1. Introduction

The Mersenne problem asks if $M_n = 2^n - 1$ is prime for infinitely many values of n. Three and a half centuries after Mersenne's death this problem remains inaccessible. In addition to their position in number theory, Mersenne primes have arisen in diverse areas of mathematics, including group theory [11], ergodic theory [26] and string theory [12]. Their properties have also led some fine minds astray [2]. Wagstaff [25] modified some considerations by Gillies [13] to produce a heuristic argument of the following shape about the distribution of Mersenne primes: If various congruences satisfied by the Mersenne numbers behave like independent probabilistic events, then the number of Mersenne primes less than X should be about

$$\frac{e^\gamma}{\log 2} \log\log X = (2.5695\ldots)\log\log X.$$

Moreover, if $n_1, \ldots, n_r$ are the primes for which M_{n_j} is prime, then the argument predicts that

$$\frac{\log\log M_{n_j}}{j} \longrightarrow \frac{\log 2}{e^\gamma}. \tag{1}$$

There is little hope that this heuristic argument could ever be tightened up to become a proof, but it is certainly suggestive. For example, plotting $\log\log M_{n_j}$ against j gives an extremely close agreement with the prediction – though it is hard to attach statistical significance to a finite sample of an infinite problem. The 39 known Mersenne primes behave very much in accordance with (1) – see the Prime Pages [3]

for the details. The reason so few Mersenne primes are known is that the rapid growth rate in the sequence $(2^n - 1)$ means that huge numbers must be tested for primality, and although the special shape of Mersenne numbers permits very rapid prime testing, even finding the first 39 has taken thousands of computers many years, running a distributed program.

2. Other settings of the Mersenne problem

One approach to the Mersenne problem is to try to see it in different contexts; several of these will be described below. A remarkable feature of the second and third of these is that for some special cases it is possible to *prove* the appearance of infinitely many primes. Our purpose here is to expand on the fourth and fifth of these, and to describe heuristic and computational evidence for the expected behaviour. There are sharp generalisations or modifications of the Mersenne problem to other specific questions (for example, see [1], [19]); we are primarily interested in naturally arising *families* of problems which may shed some light on the Mersenne problem.

2.1. **Lehmer–Pierce sequences.** Fix a monic polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$, with factorization over $\mathbb{C}$

$$f(x) = (x - \alpha_1) \dots (x - \alpha_d). \tag{2}$$

Following Pierce and Lehmer, associate a sequence of integers to f by defining

$$\Delta_n(f) = \prod_{i=1}^{d} |\alpha_i^n - 1| \text{ for } n \geq 1. \tag{3}$$

For the polynomial $f(x) = x - 2$ these are the Mersenne numbers. In any case, the resulting sequence is again a divisibility sequence, and an analogue of the heuristic arguments of Wagstaff may be applied to it (once generic divisibility is taken care of: $\Delta_n(f)$ is always divisible by $\Delta_1(f)$; if f is a reciprocal polynomial then $\Delta_n(f)/\Delta_1(f)$ is always a square when n is odd). The rate of growth of the sequence is determined by the *Mahler measure* of the polynomial f, and by choosing polynomials with small Mahler measure the growth rate of $\Delta_n(f)$ can be reduced dramatically. Lehmer [16] studied these sequences with the view of using them to produce large primes in novel ways. Recently, his approach was revisited using modern computing methods, together with the heuristic argument of Wagstaff. The upshot of this work is described in [6], where sequences have been found with many hundreds of primes, and a reasonable agreement with the heuristic model is found.

2.2. **Primes from dynamical systems.** The Lehmer–Pierce sequences all arise from algebraic dynamical systems in the following sense. Call a sequence $(u_n)_{n\geq 1}$ *algebraically realisable* if there is a compact group endomorphism $T : X \to X$ with the property that

$$u_n = |\mathrm{Per}_n(T)| = |\{x \in X \mid T^n(x) = x\}|.$$

Such a sequence must be a divisibility sequence in addition to being *realisable* (a general combinatorial notion expressing the property of being the periodic points for some map – see [20] for the details). The converse is not true, and only a partial characterization of algebraically realisable sequences is known.

Any divisibility sequence must satisfy $u_1|u_n$ for all n, but it seems reasonable to ask whether the quotient might be prime infinitely often. The Lehmer–Pierce sequences are a natural family of algebraically realizable sequences that are conjectured to be prime infinitely often (once this kind of generic divisibility is taken account of). It turns out that many other natural families of group automorphisms have a similar property: Example 2.1 shows that the even Bernoulli denominators have this property. Studying primality from this point of view gives a conjectural explanation for the infinitude of both Mersenne and Sophie-German primes within the same context. Example 2.2 gives some hope that such sequences might indeed be prime infinitely often.

Example 2.1. Let B_n be defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n t^n / n!$$

Then the sequence $b_n = \mathrm{denominator}(B_{2n})$ is algebraically realisable.

To see this, define $X_p = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. For $p = 2$ define T_p to be the identity. For $p > 2$, let g_p denote an element of (multiplicative) order $(p-1)/2$. Define $T_p : X_p \to X_p$ to be the endomorphism $T_p(x) = g_p x \mod p$. Plainly $|\mathrm{Per}_n(T_p)| = p$ if and only if $p - 1|2n$; for all other n, $|\mathrm{Per}_n(T_p)| = 1$. The Clausen–von Staudt Theorem ([14], [15]) states that

$$B_{2n} + \sum \frac{1}{p} \in \mathbb{Z},$$

where the sum ranges over the primes p for which $p - 1|2n$. Thus $|\mathrm{Per}_n(T_p)| = \max\{1, |B_{2n}|_p\}$. Now define

$$X = \prod_p X_p \text{ and } T = \prod_p T_p.$$

This shows the algebraic realisability of the Bernoulli denominators.

Notice that a prime value of b_n/b_1 can only occur if n is a Sophie-Germain prime. There are believed to be infinitely many Sophie-Germain primes but no proof is available – see [21].

The next example is a group endomorphism with a very similar shape to that of Example 2.1, but constructed so as to be certain that the periodic point sequence will be prime infinitely often. This example was inspired by a remark of Gerry McLaren.

Example 2.2. There is a group endomorphism $T : X \to X$ such that $|\mathrm{Per}_n(T)|$ takes on infinitely many distinct prime values. To see this, construct a set S of prime numbers recursively as follows. Firstly, $2 \in S$ and a prime $p \in S$ if and only if $p-1$ is divisible by a prime $q = q_p$ which does not divide $p' - 1$ for all $p' \in S$ with $p' < p$. Clearly S is infinite – otherwise all sufficiently large primes could be written as $1 + p_1^{e_1} \dots p_r^{e_r}$ for some fixed set of primes $\{p_1, \dots, p_r\}$, where $e_1, \dots, e_r$ lie in $\mathbb{N}$. The number of such primes less than or equal to X is $O((\log X)^r)$, which contradicts the Prime Number Theorem.

For each prime $p \in S$, let h_p denote an element of multiplicative order $q = q_p$ in $X_p = \mathbb{F}_p$, and define an endomorphism $T_p : X_p \to X_p$ by $T_p(x) = h_p x$. Then define an endomorphism T on X by

$$X = \prod_{p \in S} X_p \text{ and } T = \prod_{p \in S} T_p.$$

Clearly $|\mathrm{Per}_{q_p}(T)| = p$ for all p, showing that the sequence $(|\mathrm{Per}_n(T)|)$ takes on infinitely many distinct prime values.

2.3. **Mersenne problem in A-fields.** Let k be an $\mathbb{A}$-field (that is, an algebraic number field or a finite extension of a rational function field $\mathbb{F}_q(t)$ of positive characteristic) with set of places $\mathbb{P}(k)$ (see [28] for a discussion of places). Fix $\xi \in k \backslash \{0\}$, not a unit root. Then the generalized Mersenne problem asks if there is a constant $B(\xi)$ with the property that the set

$$P_n = \{\nu \in \mathbb{P}(k) \mid |\xi^n - 1|_\nu \neq 1\}$$

has no more than $B(\xi)$ elements for infinitely many n. For $k = \mathbb{Q}$ and $\xi = 2$, this is a weak form of the classical Mersenne problem (in that it only asks for infinitely many numbers $2^n - 1$ to have a uniformly bounded number of prime factors). This problem has arisen in ergodic theory [26], [27] and has the following remarkable feature: There are many cases for which it is certainly true, though the proofs are not trivial. Specifically, a consequence of Heath–Brown's work on the Artin conjecture is that $|P_n| = 2$ infinitely often for many of the positive characteristic cases (see [27] for the details).

3. A Higher-rank Mersenne problem

The dynamical systems alluded to above have very natural higher-rank analogues, namely the $\mathbb{Z}^d$-actions generated by d commuting automorphisms of a compact abelian group X (see [18], [22] for a discussion of these dynamical systems). For these the periodic point behaviour is very complicated (some of these problems are described in [17] in a different context), and we simply extract one simple question from the simplest example available. Does the set

$$\{3^m 2^n - 1 \mid m, n \geq 0\}$$

contain infinitely many primes? Can anything be said – even heuristically – about the quantity

$$N^-(X) = |\{(m,n) \mid 3^m 2^n - 1 \text{ is prime and } m, n \leq X\}|? \tag{4}$$

This problem will be discussed in this section, along with the same question for the quantity $N^+(X)$ associated to $3^m 2^n + 1$, which is quite different in that it certainly does not come from a pair of commuting group automorphisms.

3.1. **Heuristics.** The heuristic argument below takes the form of a family of successive refinements of the same basic idea. Let $N^-(X)$ be defined by (4). In the discussion below, we will essentially ignore the cases $n = 0$ (for which $3^m 2^n - 1$ is always even) and $m = 0$ (the Mersenne case) since they together contribute so few primes. The discussion leads to a prediction that

$$\frac{N^-(X)}{X} \to C^- \text{ as } X \to \infty, \tag{5}$$

where C^- is a constant. The section ends with a graph to illustrate the accuracy of the prediction. We will also exhibit a graph for primes of the form $3^m 2^n + 1$.

The Prime Number Theorem implies that the probability a large random integer K is prime is approximately $\frac{1}{\log K}$. This suggests that $N^-(X)$ is approximately

$$N_1(X) = \sum_{1 \leq m,n < X} \frac{1}{n \log 2 + m \log 3} \tag{6}$$

which is given asymptotically by the double integral

$$\int_1^X \int_1^X \frac{1}{x \log 2 + y \log 3} \, \mathrm{d}x \, \mathrm{d}y,$$

so

$$N_1(X) = DX + O(\log X),$$

where

$$D = \frac{\log 6 \log\log 6 - \log 2 \log\log 2 - \log 3 \log\log 3}{\log 2 \log 3} = 1.57\ldots .$$

3.2. **Obvious congruences.** For $m, n \geq 1$, $3^m 2^n - 1$ is coprime with 6. The usual Euler factor correction suggests that we should therefore increase our estimate for $N^-(X)$ by a factor of $\frac{2}{2-1} \cdot \frac{3}{3-1} = 3$. This gives a refined heuristic: Having taken account of the Prime Number Theorem and the primes 2 and 3, we expect $N^-(X)$ to be approximated by $N_2(X)$, where

$$\frac{N_2(X)}{X} \sim 4.71\ldots$$

3.3. **Less obvious congruences.** It is tempting to continue exactly as above. Consider the prime $q = 5$ and the congruence

$$3^m 2^n - 1 \equiv 0 \bmod 5.$$

The solutions are all the pairs (m, n) which reduce mod 4 to lie in the set $\{(1,1),(2,2),(3,3),(4,4)\}$. Thus asymptotically $\frac{3}{4}$ of the numbers of the form $3^m 2^n - 1$ are not divisible by 5; on the other hand $\frac{4}{5}$ of all numbers are not divisible by 5. This suggests that the heuristic estimate taking account of the prime 5 as well should be $\frac{5}{4} \cdot \frac{3}{4} \cdot N_2(X)$, leading to the estimate

$$\frac{N_3(X)}{X} \sim 4.416\ldots .$$

It is at this point that the first substantial difficulty is encountered. The proportion of numbers of the form $3^m 2^n - 1$ that are not divisible by 5 or 7 cannot be found by emulating this calculation mod 4 and 6 separately – we have to search in residue classes mod $12 = \mathrm{lcm}(4, 6)$.

3.4. **Taking account of primes less than L.** The calculation to find the correcting factor for primes q, $3 < q < L$, goes as follows. Let P_L denote the least common multiple of $q - 1$ as q runs over the primes between 3 and L. For each residue pair (j, k) in $(\mathbb{Z}/P_L\mathbb{Z})^2$, and for each such prime q, reduce (j, k) mod q and decide whether

$$3^j 2^k - 1 \equiv 0 \bmod q.$$

Delete those residue pairs that satisfy this congruence for some q; call the remaining set Q_L. Then the heuristic argument suggests that we should correct by this factor and the usual Euler factor to give

$$N_L(X) = \frac{|Q_L|}{P_L^2} \cdot \prod_{3<q<L} \frac{q}{q-1} \cdot N_2(X).$$

This has two distinct pieces: the second factor is readily estimated using Merten's Theorem [14, Th. 429] which says that

$$\frac{1}{\log L}\prod_{2\le q<L}\frac{q}{q-1}\to e^{\gamma},\ \text{as } L\to\infty.$$

The other factor presents computational and theoretical problems: Computationally, P_L grows very rapidly in L, and the exact calculation of $|Q_L|$ requires manipulating set-memberships which is slow. However, approximations can be made easily by simple counting arguments. It is possible that results on the higher-rank Artin problem (conditional on GRH) would give more precise information, but we have not pursued this as Q_L already arises inside a heuristic argument.

3.5. **A comparison of heuristic and experimental evidence.** As described above, calculating exact values for $|Q_L|$ involves searching over a set of size P_L^2 (for primes up to $L=29$, a calculation over a set of size 55440^2 is involved). Bearing in mind the sometimes delicate balance between computation time and accuracy of results we fix L and estimate $|Q_L|/P_L^2$ by counting the number of pairs (m,n) with $m,n<X$ and $\gcd(2^m3^n-1,\prod_{p<L}p)>1$, then divide by X^2. Experiments suggest that for given L this converges rapidly in X, and a good approximation is found even when X is of the order of L. For $L=1000$ the calculation suggests the further refined heuristic

$$\frac{N_L(X)}{X}\sim 4.043\ldots$$

The experimental evidence strongly supports a conjecture of the form (5), which suggests that

$$\log L\cdot\frac{|Q_L|}{P_L^2}$$

converges as $L\to\infty$. Figure 1 shows a graph of the number $N^-(X)$ of primes of the form 3^m2^n-1 with $m,n<X$ against X for values of $X\le 1000$. The gradient of this graph is approximately $C^-=3.7$, as compared with our most refined heuristic suggestion of $C^-=4.043\ldots$. However, the conjectured linearity is strongly supported by this numerical data.

Much of what we have said for primes of the form 3^m2^n-1 can be replicated for primes of the form 3^m2^n+1. That is to say, the heuristic argument above can be applied in this case also, taking into account the possible difference in the value of $|Q_L|/P_L^2$. Let $N^+(X)$ denote the

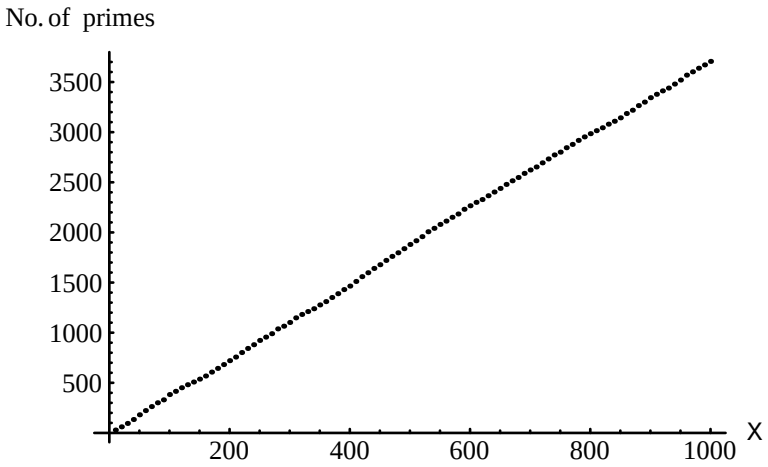

FIGURE 1. Graph of $N^-(X)$ against X for $X \leq 1000$

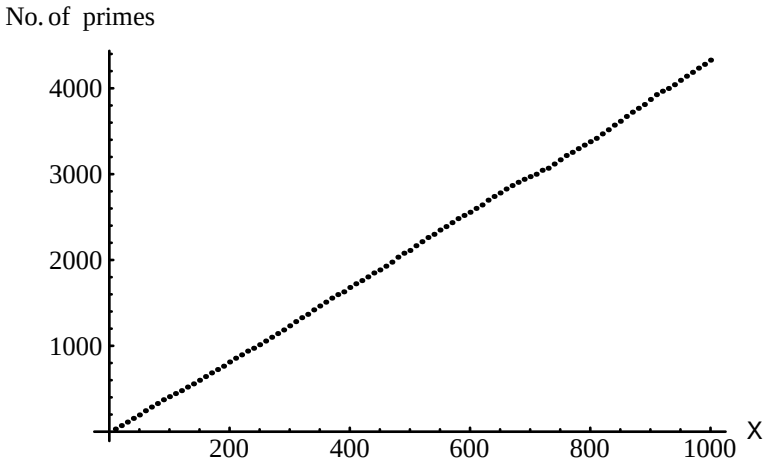

FIGURE 2. Graph of $N^+(X)$ against X for $X \leq 1000$

number of primes of the form $3^m 2^n + 1$ with $m, n \leq X$. We expect

$$\frac{N^+(X)}{X} \to C^+, \text{ as } X \to \infty.$$

Figure 2 shows a graph of $N_+(X)$ against X for $X \leq 1000$.

The graph predicts the value of C^+ to be about 4.3. Comparing this with a refined heuristic calculated in an identical fashion to that above, we obtain

$$\frac{N_L^+(X)}{X} \sim 4.258\ldots$$

with $C^+ = 4.258$. This heuristic constant is *extremely* close to the experimental value, though no meaning can attach to this coincidence in light of the N^- case.

4. Elliptic analogues

There is a dialogue between on the one hand dynamical systems and arithmetical sequences built from the circle (of which the Lehmer–Pierce sequences are the simplest example) and on the other, objects associated to elliptic curves, summarised in Table 1 (the objects on the classical side are described in [10], and on the elliptic side in [8] and [9]).

classical case	elliptic case
polynomial $f \in \mathbb{Z}[x]$	point P on curve E over $\mathbb{Q}$
Mahler measure $m(f)$	canonical height $h_E(P)$
Lehmer problem	Lang's height conjecture
toral automorphism T_f	sequence of maps
$(\lvert\mathrm{Per}_n(T_f)\rvert)$ (Lehmer–Pierce)	elliptic divisibility sequence

Table 1. Classical objects and their elliptic counterparts

Let E denote an elliptic curve defined over the rationals (the text [24] covers all the properties of elliptic curves we use), given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{7}$$

with coefficients $a_1, \ldots, a_6 \in \mathbb{Z}$. The assumption that the curve is an elliptic curve amounts to assuming it is non-singular, that is, the discriminant does not vanish.

How might we expect to use the arithmetic of E to produce primes? Suppose E has a non-torsion rational point $Q \in E(\mathbb{Q})$. The multiples nQ for $n \in \mathbb{N}$ define a sequence of integers as follows: The x-coordinates of these points all have the shape $x(nQ) = t_n/s_n^2$ for integers s_n, t_n. These fascinating sequences were studied in [23]. We could ask whether they are likely to contain many primes - actually, it is sufficient to study s_n. The Chudnovskys did some experimental research in the 80's (see [4] and [5]) and produced some quite large prime values of s_n. Their results have been revisited recently (see [7]) in work that suggests the sequence s_n will only contain *finitely* many primes. Indeed, the sequences in [4] do not produce any additional primes when tested over a much larger range.

It seems very likely that working with translations $P + nQ$ for fixed rational points P and Q would produce similar results. Our heuristic argument depends heavily upon the growth rate of the sequence, and this would not be substantially different for nQ or $P + nQ$.

Suppose now that $E(\mathbb{Q})$ has rank > 1, and choose independent non-torsion points P and Q. Let $s(m, n) \in \mathbb{Z}$ be defined by

$$x(mP + nQ) = t(m, n)/s(m, n)^2. \tag{8}$$

In his PhD thesis the second author gives a heuristic argument, accompanied by much data, to suggest that $s(m, n)$ should take on prime values infinitely often. Indeed, the number of prime values with $|m|, |n| < X$ should be asymptotically $c \log X$, where c is a constant depending upon the finer arithmetic of E. The elliptic regulator (see below) appears in an apparently explicable fashion although the constant is also affected by the finer divisibility properties in a way that is hard to fathom. The sequences $s(m, n)$ provide large primes which can be described unambiguously in a very economical fashion, since $s(m, n)$ grows as the exponential of a positive-definite quadratic form in the variables m and n.

4.1. **Heuristics in the elliptic case.** Let $R_X = \{(m, n) \mid |m|, |n| \leq X\}$. Then the first attempt at a heuristic estimate is that the sum

$$\sum_{R_X} 1/\log s(m, n) \tag{9}$$

is the expected number of prime values of $s(m, n)$ with $(m, n) \in R_X$. Now $\log s(m, n)$ is asymptotically equivalent to a positive definite quadratic form $S(m, n)$, and the asymptotics of the sum

$$\sum_{R_X} 1/S(m, n)$$

are well known: This sum is asymptotically $(2\pi/r) \log X$, where r denotes the determinant of S (r is the *elliptic regulator* of P and Q). This asymptotic arises from comparing the sum with a suitable integral.

As before, this estimate needs refinement. If q denotes any prime then the sequence reduced mod q is periodic in both variables, with period dividing $|E(\mathbb{F}_q)|$. If follows that we can assign a (rational) probability to $s(m, n)$ not being divisible by q. Doing this for the primes $q < L$ gives approximately $c_L X^2$ elements (m, n) in R_X for which $s(m, n)$ is not divisible by primes less than L. Letting $L \to \infty$, we expect approximately $e \log X$ primes, where e depends on E but not X. It is computationally *extremely* difficult to calculate the exact

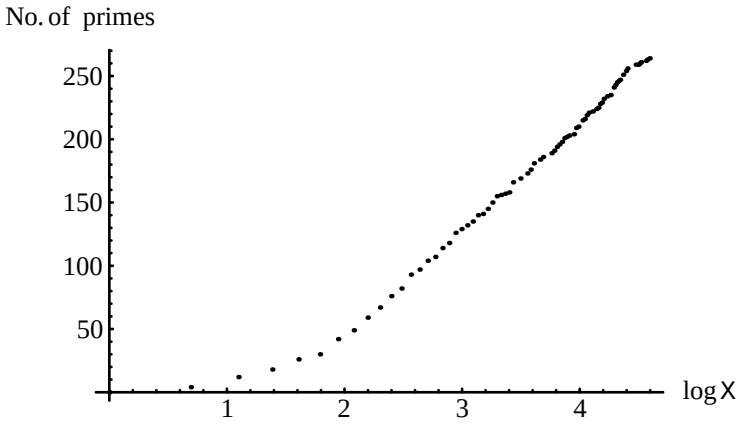

FIGURE 3. Graph of $N_E(X)$ against $\log X$ for $X \leq 100$; curve $y^2 + y = x^3 - 199x + 1092$

probabilities for various L, but as before approximations via counting arguments are not too difficult to obtain.

4.2. **Numerical data.** Figures 3 and 4 show graphs for $N_E(X)$, the number of primes $s(m, n)$ with $|m|, |n| \leq X$ against $\log X$ for two rank-2 elliptic curve E with small regulator.

The curve in Figure 3 is

$$y^2 + y = x^3 - 199x + 1092,$$

with independent rational points $P = (-13, 38)$ and $Q = (-6, 45)$ on the curve, whose regulator is $.0360\ldots$

The curve in Figure 4 is

$$y^2 + y = x^3 - 28x + 52,$$

with independent rational points $P = (-4, 10)$ and $Q = (-2, 10)$ on the curve, whose regulator is $.0813\ldots$

The numerical data is not incompatible with the heuristic suggestion of a linear relationship between $N_E(X)$ and $\log X$, but strongly suggests there are more phenomena here to understand.

5. CONCLUSION

The classical Mersenne problem appears as a special case in many different settings. In some of these there are other cases in which prime appearance is understood. Two higher-rank analogues of the Mersenne problem are explored.

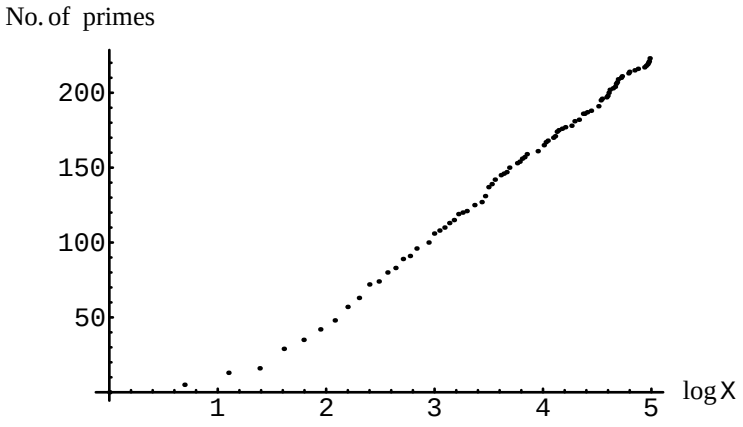

FIGURE 4. Graph of $N_E(X)$ against $\log X$ for $X \leq 150$; curve $y^2 + y = x^3 - 28x + 52$

The first is a direct extension to two variables, and compelling numerical data is available concerning prime appearance.

The second occurs in an elliptic curve setting. The work of [7] suggests there are only finitely many primes in an elliptic divisibility sequence (and possibly a uniform bound on the number of primes for any elliptic divisibility sequence on curves defined over the rationals). A better elliptic analogue of the Mersenne problem therefore seems to be the study of the higher-rank sequences associated to elliptic curves of higher rank.

REFERENCES

[1] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, Jr. The new Mersenne conjecture. *Amer. Math. Monthly*, 96(2):125–128, 1989.

[2] P. G. Brown. A note on Ramanujan's conjectures regarding "Mersenne's primes". *Austral. Math. Soc. Gaz.*, 24(4):146–147, 1997.

[3] Chris Caldwell. The prime pages. `http://www.utm.edu/research/primes/`.

[4] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7(4):385–434, 1986.

[5] D. V. Chudnovsky and G. V. Chudnovsky. Computer assisted number theory with applications. In *Number theory (New York, 1984–1985)*, pages 1–68. Springer, Berlin, 1987.

[6] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in sequences associated to polynomials (after Lehmer). *LMS J. Comput. Math.*, 3:125–139 (electronic), 2000.

[7] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.*, 4:1–13 (electronic), 2001.

[8] Manfred Einsiedler, Graham Everest, and Thomas Ward. Entropy and the canonical height. *J. Number Theory*, 91:256–273, 2001.
[9] Graham Everest and Thomas Ward. A dynamical interpretation of the global canonical height on an elliptic curve. *Experiment. Math.*, 7(4):305–316, 1998.
[10] Graham Everest and Thomas Ward. *Heights of polynomials and entropy in algebraic dynamics*. Springer-Verlag London Ltd., London, 1999.
[11] Shalom Feigelstock. Mersenne primes and group theory. *Math. Mag.*, 49(4):198–199, 1976.
[12] Paul H. Frampton and Thomas W. Kephart. Mersenne primes, polygonal anomalies and string theory classification. *Phys. Rev. D (3)*, 60(8):087901, 4, 1999.
[13] Donald B. Gillies. Three new Mersenne primes and a statistical theory. *Math. Comp.*, 18:93–97, 1964.
[14] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.
[15] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. Springer-Verlag, New York, second edition, 1984.
[16] D.H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math.* 34 (1933) 461–479.
[17] D. A. Lind. A zeta function for $\mathbb{Z}^d$-actions. In *Ergodic theory of $\mathbb{Z}^d$ actions (Warwick, 1993–1994)*, pages 433–450. Cambridge Univ. Press, Cambridge, 1996.
[18] Douglas Lind, Klaus Schmidt, and Tom Ward. Mahler measure and entropy for commuting automorphisms of compact groups. *Invent. Math.*, 101(3):593–629, 1990.
[19] Albert A. Mullin. Letter to the editor: "The new Mersenne conjecture" [Amer. Math. Monthly **96** (1989), no. 2, 125–128; MR 90c:11009] by P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr. *Amer. Math. Monthly*, 96(6):511, 1989.
[20] Yash Puri and Thomas Ward. Arithmetic and growth of periodic orbits. *J. Integer Seq.*, 4(1):Article 01.2.1, 17 pp. (electronic), 2001.
[21] J. H. Sampson. Sophie Germain and the theory of numbers. *Arch. Hist. Exact Sci.*, 41(2):157–161, 1990.
[22] Klaus Schmidt. *Dynamical systems of algebraic origin*. Birkhäuser Verlag, Basel, 1995.
[23] Rachel Shipsey. *Elliptic Divisibility Sequences*. PhD thesis, University of London, 2003.
[24] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
[25] Samuel S. Wagstaff, Jr. Divisors of Mersenne numbers. *Math. Comp.*, 40(161):385–397, 1983.
[26] Thomas Ward. An uncountable family of group automorphisms, and a typical member. *Bull. London Math. Soc.*, 29(5):577–584, 1997.
[27] Thomas Ward. Almost all S-integer dynamical systems have many periodic points. *Ergodic Theory Dynam. Systems*, 18(2):471–486, 1998.
[28] André Weil. *Basic number theory*. Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, U.K., *E-mail address*, G.Everest@uea.ac.uk: ,

, WWW HOME PAGE: HTTP://WWW.MTH.UEA.AC.UK/PEOPLE/GRE.HTML